

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

PAIGE A. THOMPSON,

Defendant.

Case No. CR19-159-RSL

ORDER GRANTING IN
PART MOTION TO SEAL
AND REDACT ADMITTED
TRIAL EXHIBITS

This matter comes before the Court on the government's "Motion to Seal and Redact Admitted Trial Exhibits" (Dkt. # 353). Having reviewed the submissions of the parties and the remainder of the record, the Court finds as follows:

I. Background

On June 17, 2022, following an eight-day trial, a jury convicted defendant of (i) one count of wire fraud, in violation of 18 U.S.C. § 1343, (ii) one count of unlawfully obtaining information of a card issuer, in violation of 18 U.S.C. § 1030(a)(2), (iii) four counts of unlawfully obtaining information from a protected computer, in violation of 18 U.S.C. § 1030(a)(2), and (iv) one count of transmitting a program, information, code, or command to a computer, intending to cause damage, in violation of 18 U.S.C. § 1030(a)(5). Dkt. # 335.

In the Western District of Washington, following a jury verdict, the parties are required to file a set of admitted exhibits reviewed by the trier of fact. General Order No. 01-18, *In re Exhibits Retention Procedures* (W.D. Wash. Jan. 18, 2018) at ¶ 9. Any confidential exhibits admitted at trial may be filed under seal utilizing the Court's existing methods for filing documents under seal. *Id.* at ¶ 10. The government seeks to seal and redact certain exhibits.

ORDER GRANTING IN PART MOTION TO SEAL
AND REDACT ADMITTED TRIAL EXHIBITS - 1

II. Discussion

The First Amendment protects the public's right of access to criminal trials. See Globe Newspaper Co. v. Superior Ct. for Norfolk Cnty., 457 U.S. 596, 606 (1982). The public also has a common law right to inspect and copy public records, including those from judicial proceedings. See Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978). In light of these rights, closure is appropriate "only if three substantive requirements are satisfied: (1) closure serves a compelling interest; (2) there is a substantial probability that, in the absence of closure, this compelling interest would be harmed; and (3) there are no alternatives to closure that would adequately protect the compelling interest." United States v. Doe, 870 F.3d 991, 998 (9th Cir. 2017) (quoting Oregonian Publ'g Co. v. U.S. Dist. Ct. for Dist. of Or., 920 F.2d 1462, 1466 (9th Cir. 1990)); see also Times Mirror Co. v. United States, 873 F.2d 1210, 1211 n.1 (9th Cir. 1989). "The court must not base its decision on conclusory assertions alone, but must make specific factual findings." Id. (quoting Oregonian, 920 F.2d at 1466).

The government moves the Court to seal or redact three categories of exhibits: (A) personal identifying information and account numbers, (B) victims' role names and file structures and lists, and (C) defendant's code. The Court considers each category in turn.

A. Personal Identifying Information and Account Numbers

The government first moves the Court to redact personal identifying information and account numbers. See Dkt. # 353 at 3-6. Defendant agrees that redaction of this information is generally appropriate and consents to sealing Exhibit 506, which includes such information.¹ See Dkts. # 359 at 1, # 353-2 at 11-12 (Exhibit 506). Redaction of personal identifying information and account numbers is required under Local Rule 49.1(a). See Local Rules W.D. Wash. CrR 49.1(a) (listing personal data identifiers required to be redacted in all documents filed with the Court). The government's motion to redact personal identifying information and account numbers is therefore granted.

¹ The Court notes that while defendant does not oppose sealing Exhibit 506, the government does not seek to seal Exhibit 506. Rather, the government moves to redact a victim's date of birth, address, and phone number contained therein. See Dkts. # 353 at 5, # 353-2 at 11-12.

1 **B. Victims' Role Names and File Structures and Lists**

2 The government next moves the Court to order redaction or sealing of the victims' role
3 names and file structures and lists. See Dkt. # 353 at 3-6. Defendant's response memorandum
4 indicates that she does not oppose sealing Exhibit 731, which includes "a victim's role name and
5 reveals the victim's cloud-computing server and file structure," but does not otherwise address
6 this request. See Dkts. # 353 at 4, # 359 at 1.

7 The Court finds that exhibits containing victim role names and file structures and lists are
8 properly redacted or sealed, as appropriate, as confidential business information. First, other
9 district courts applying the compelling reasons standard have sealed confidential business
10 information that renders an entity more susceptible to malware attack if such information is
11 made public. See, e.g., Adtrader, Inc. v. Google LLC, No. 17-CV-07082-BLF, 2020 WL
12 6391210, at *2 (N.D. Cal. Mar. 24, 2020) (finding compelling reasons to seal portions of
13 document containing "highly sensitive, confidential information about the functionality of
14 Google's systems used to detect and react to invalid activity, including information about
15 Google's policies and specific webpages that are perpetrators of ad fraud and distributors of
16 malware," disclosure of which "could cause competitive harm to Google by revealing to
17 competitors and bad actors the capabilities of Google's systems," and "make it easier to
18 circumvent or evade Google's detection systems."); Reyna v. Arris Int'l PLC, No. 17-CV-
19 01834-LHK, 2018 WL 1400513, at *3 (N.D. Cal. Mar. 20, 2018) (acknowledging that "detailed
20 information about the technology that a company uses to protect against hacking and other types
21 of attacks, or specific vulnerabilities in that technology, is sealable under the compelling reasons
22 standard"). This supports the conclusion that closure of confidential business information of
23 this sort serves a compelling interest.

24 Second, a victim testified that disclosure of this information would render it more
25 susceptible to attack. See Dkt. # 353 at 4. This supports the conclusion that there is a
26 substantial probability that, in the absence of closure, the relevant compelling interest would be
27 harmed. Further, the "presumption of access may be overcome only 'on the basis of articulable
28 facts known to the court, not on the basis of unsupported hypothesis or conjecture.'" Hagestad

1 v. Tragesser, 49 F.3d 1430, 1434 (9th Cir. 1995). This victim’s testimony provides articulable
 2 facts known to the Court and elevates the risk beyond mere hypothesis or conjecture. The
 3 government’s motion to redact or seal the victims’ role names and file structures and lists is
 4 therefore granted. To ensure that there are no alternatives to closure that would adequately
 5 protect the compelling interest, the information shall be redacted unless the exhibit in question
 6 contains so much sensitive material that redaction is impracticable, in which case it shall be
 7 sealed.

8 **C. Defendant’s Code**

9 Finally, the government moves the Court to seal defendant’s code on the ground that
 10 copycat criminals could attempt to use the code to hack the computers of the same or new
 11 victims. See Dkt. # 353 at 2. Defendant objects on the grounds that the government has offered
 12 no bases to suggest there is a substantial probability that another person will copy defendant’s
 13 code or that there are no alternatives to sealing that would adequately protect companies
 14 utilizing AWS servers, sealing would be inconsequential because the code has already been
 15 widely disseminated in the tech community, and public access to defendant’s code would clarify
 16 Computer Fraud and Abuse Act (“CFAA”) caselaw. See Dkt. # 359 at 2-5.

17 Defendant’s code should remain unsealed. First, hypothesis or conjecture is insufficient
 18 to overcome the presumption of access. Hagestad, 49 F.3d at 1434. The government’s
 19 argument that it “simply defies belief” to think that a copycat will not attempt to mimic
 20 defendant’s actions, see Dkt. # 361 at 2, amounts to hypothesis or conjecture. It is therefore
 21 insufficient to meet the government’s burden to justify sealing. Cf. Doe, 870 F.3d at 999-1000
 22 (relying on CCACM Report to support sealing based on danger to inmates who receive § 5K1.1
 23 downward departure for substantial assistance); Dugan v. Lloyds TSB Bank, PLC, No. 12-CV-
 24 02549-WHA (NJV), 2013 WL 1283435, at *7-8 (N.D. Cal. Mar. 26, 2013) (denying motion to
 25 seal bank’s internal funding mechanism “in the age of increasing cyber-attacks that can wreak
 26 havoc on financial institutions” where bank failed to provide a declaration or other specific
 27 evidence supporting this threat). It is not defendant’s burden to show that a copycat attack will
 28 not occur, but rather the government’s burden to provide some evidence that it might. See

1 Kamakana v. City & Cnty. of Honolulu, 447 F.3d 1172, 1178 (9th Cir. 2006) (“A party seeking
2 to seal a judicial record then bears the burden of overcoming [the] strong presumption [in favor
3 of access] by meeting the ‘compelling reasons’ standard.”). The government has not met this
4 burden.

5 Second, the government has failed to show that there are no alternatives to sealing that
6 would adequately protect companies utilizing AWS servers. Given the “strong presumption of
7 openness,” closure is appropriate only where it “is necessitated by a compelling governmental
8 interest” and “is narrowly tailored to serve that interest.” Doe, 870 F.3d at 997 (quoting Times
9 Mirror Co., 873 F.2d at 1211 n.1); see also Finjan, Inc. v. Blue Coat Sys., LLC, No. 15-CV-
10 03295-BLF, 2017 WL 1540640, at *1 (N.D. Cal. Apr. 28, 2017) (denying motion to seal
11 documents “contain[ing] highly confidential technical information regarding Blue Coat’s
12 proprietary technology, and confidential aspects of Blue Coat’s business,” disclosure of which
13 “would create substantial risk of serious harm to Blue Coat, including evasion of Blue Coat’s
14 malware analysis tools, disclosure to competitors regarding the scanning tools used in the
15 accused products, and Blue Coat’s approach to fixes in the products” because request to seal
16 documents in their entirety was not narrowly tailored). Sealing central evidence in its entirety is
17 not a narrowly tailored approach, particularly in the absence of an explanation regarding why a
18 less sweeping alternative, such as redaction, does not suffice.

19 Third, in analyzing whether compelling reasons justify sealing computer code, district
20 courts often consider its centrality. See, e.g., In re Yahoo! Inc. Customer Data Sec. Breach
21 Litig., No. 16-MD-02752-LHK, 2018 WL 9651897, at *3 (N.D. Cal. Jan. 3, 2018) (“[I]t does
22 not appear that the redacted information is integral to the substantive issue of Yahoo’s liability,
23 as Plaintiffs do not recite the redacted information within any of the specific causes of action . . .
24 However, if some of the redacted information is later important to a motion that is more than
25 tangentially related to the merits, it may be the case that the reasons to seal do not outweigh the
26 public interest in disclosure.”); In re Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013
27 WL 5366963, at *3 (N.D. Cal. Sept. 25, 2013) (sealing information about the Gmail system
28 based on Google’s assertions that “hackers and spammers could use this information to

1 circumvent Google’s anti-virus and anti-spam mechanisms” and in light of the absence of a
2 “strong public interest in disclosure of the material . . . since this material is unlikely to be
3 critical to the substantive issue of liability.”); Music Grp. Macao Com. Offshore Ltd. v. Foote,
4 No. 14-CV-03078-JSC, 2015 WL 3993147, at *5-6 (N.D. Cal. June 30, 2015) (sealing
5 information regarding systems and servers in cyberattack case but cautioning that “[i]t may well
6 be that, as this case progresses the balance shifts in favor of disclosure. In particular, if evidence
7 of Plaintiff’s systems and servers is offered at trial to support Plaintiff’s claims that Defendant
8 failed to protect those systems or could have done more to mitigate the effects of a cyber attack,
9 the public’s interest in disclosure may outweigh Plaintiff’s concerns about preventing future
10 attacks.”). Defendant’s code is undisputedly central to her conviction. This weighs in favor of
11 public access.

12 Lastly, the bulk of the government’s reply memorandum is dedicated to rebutting
13 defendant’s contentions that sealing would be inconsequential because the code has already been
14 widely disseminated in the tech community and that public access to defendant’s code would
15 clarify CFAA caselaw. See Dkt. # 361 at 2-4. The Court agrees that general articles regarding
16 the hack and AWS guides do not demonstrate that defendant’s code is already broadly known.
17 See Dkt. # 359 at 3 (citing articles and guides); see also Dkt. # 361 at 2-3 (government’s
18 argument). While pre-existing dissemination may go to whether there is a substantial
19 probability that, in the absence of closure, a compelling interest would be harmed, see Doe, 870
20 F.3d at 998, this is not dispositive. It is the government’s burden to show the substantial
21 probability of harm, not defendant’s burden to show that harm will not occur. See Kamakana,
22 447 F.3d at 1178. The government’s assertion that viewing the code would not aid in the
23 development of CFAA caselaw also fails. Again, the strength of defendant’s argument is
24 inconsequential because it is the government’s burden to carry. Further, the Court is skeptical of
25 the government’s argument. CFAA caselaw is murky and evolving. While access to the code
26 may not be useful to the average attorney, it may prove educational to industry experts.

III. Conclusion

For all of the foregoing reasons, IT IS HEREBY ORDERED that the government's Motion to Seal and Redact Admitted Trial Exhibits (Dkt. # 353) is GRANTED IN PART. The parties shall treat the disputed trial exhibits as set forth in the table below:²

| <u>Exhibit(s)</u> | <u>Treatment</u> |
|-------------------|--|
| 204-205 | Redact victim role names and file lists. |
| 252 | Redact victim role names and file lists. |
| 455 | Redact victim Amazon account numbers to last four digits. |
| 461 | Remain unsealed. |
| 506 | Redact victim date of birth, address, and phone number. |
| 608 | Redact victim role names. |
| 640 | Redact victim role names and Amazon account numbers to last four digits. |
| 643 | Redact victim role names and Amazon account numbers to last four digits. |
| 644-647 | Redact victim role names. |
| 670 | Remain unsealed. |
| 674-677 | Redact victim role names. |
| 731 | Seal. |
| 803 | Redact victim role names. |
| 804 | Redact victim role names. |
| 806-812 | Redact victim role names and Amazon account numbers to last four digits. |
| 901-904, 914-922 | Redact bank account numbers to last four digits and victim Amazon account numbers to last four digits. |
| 956 | Redact victim role names and Amazon account numbers to last four digits. |

DATED this 19th day of September, 2022.



Robert S. Lasnik
United States District Judge

² The parties may make further redactions agreed among them and consistent with this Order.